

2022

Traffic Data Ecosystem – Code of Conduct

FEBRUARY 1, 2022

1 Code of Conduct

1.1 Introduction

This Code of Conduct should not be seen as a way to restrict the actors of a data ecosystem but instead as a set of commonly acceptable norms that make cooperation between members more convenient by setting the direction for more detailed rules defined by implementing organisations. The code is not an obstacle. Like laws, it helps to create trust in a data network, which is needed for gaining real benefits and new business opportunities. This code of conduct is based on the respect between different stakeholders, transparent communication and ambition to seek the values that are commonly acceptable.

Acting ethically is not a mere cost but possibility for a resilient business.

1.2 Ethical Basis and Shared values of the Data Network

The purpose of this code is to approach the topic from the practitioners' point of view and to provide conceptual and analytical tools for assessing reasons on the basis of which the question "what should we do?" can be answered. This is done by presenting the values seen as important for data economy as well as by offering the maturity model (see next section) which can be employed in the analysis of the state of affairs in an organisation and consequently in the search of ways of improvement and development..

The following values have been found to be important in the research conducted during the IHAN project. In order the aim of fair data use to be achieved these values should be noted and respected in everyday practises..

1.2.1 Accountability and Auditability

The members of the data network are responsible for what they do, and they must be able to give satisfactory reasons for it. This means that all actors are expected to follow the Rule Book of the data network and especially its contract. All the contracts also should follow the Code of Conduct and the Rulebook of this data network. The responsibility is towards members of the data network, but also the external stakeholders – e.g., individuals, whose personal data may be processed in the data network. The operations within the data network must be reported in a comprehensive way.. Therefore, the members' records, logs and documents on data processing are suggested to be well-organized and complete, their personnel are transparent in their dealings with their auditors, and the members have a good system of internal control, security and documentation in relation to data processing.

1.2.2 Avoid harm

All actors in the data network should avoid causing harm but instead focus on creating value (direct or indirect) for the whole data network and all the people that are affected by the actions of this data network.

1.2.3 Justified Processing of Personal Data

Personal data shall be processed on a fair and lawful basis, like for example on the basis of an informed consent of the individual, in accordance with a contract with the individual, a legal obligation, a vital interest of the individual, in the public interest, or for the purposes of the legitimate interests, given that the interests and fundamental rights and freedoms of the individual are not threaten, in particular where the individual is a child.

1.2.4 Fairness, justice, and equality

All actors in the data network should promote fairness, justice, and equality among individuals. Fairness means that everyone is treated with respect regardless of their socio-economical background or status. Likewise, the benefits (economical and others) must be balanced between all stakeholders in such a manner that individuals that are the source of data are not seen as mere exploitable resources.

To ensure fair use of their information, individuals are granted true possibilities to understand and control their personal data that are collected, transferred and otherwise processed in the data network.

The rules and the structure of the data network secure the benefits and rightful expectations of all the parties. This requires a balanced power structure in the data network and transparent consensus-oriented governance.

1.2.5 Human-centricity

People live in different environments and they have personal lived experiences of their own life. They must be respected and empowered. This means that individuals have to be seen and treated as active actors with opportunities to make their own choices in the data network. They must be able to keep full and effective self-determination. Furthermore, their needs and wishes should be taken account instead of reducing them as objects or subjects.

1.2.6 Privacy

Privacy is one of the central issues in data economy. Therefore, privacy must be respected and protected. The data network is based on the use of information, which sets high demands for privacy as information can be sensitive and private. Thus, this means that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individuals. Personal data shall be collected for specified, explicit and legitimate purposes and it shall not be processed further in a manner that is incompatible with those purposes. Only personal data, which are adequate, relevant and limited to what is necessary in relation to the expressed purposes, shall be processed. Organizations do not collect personal information that they do not need. All the personal data that are processed have to be necessary for the specific use. The members of the data network take reasonable measures to ensure that personal data are accurate and up to date. Personal data must not be stored longer than necessary for the purposes for which the personal data is processed. To ensure the integrity and confidentiality of privacy, personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. To preserve the integrity, confidentiality and availability of the data, organizations are encouraged to develop and implement an information security policy framework. When merging data sets, privacy should be guarded even more carefully than normally. Anonymization of data is recommendable, whenever feasible. Any organization must also be accountable, i.e., it needs to be able to demonstrate its compliance with the principles mentioned above. Therefore, the processing of personal data must be planned and documented. There should exist clear, documented processes for data collection, storage, use, and distribution. For collected data, there needs to be a clearly documented lifecycle plan where the collection, archiving and possible erasing of data are described. The relevant parts of the lifecycle plan are available to data providers and individuals related to the data.

1.2.7 Security

All the members of the data network are responsible that their collection, use, storage, sharing, and other processing of data are secure. This means that proper security solutions and processes are used and also that monitoring, patching, and reporting of security issues are properly designed. Personal data on individuals must be properly secured and the risks to the rights and freedoms of individuals should be analysed. All the necessary technical, organisational and personal actions must be implemented to minimise security threats to individuals whose information is processed. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, all the members of the data network shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Likewise, data breaches must be responded without delays. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the responsible member of the data network shall communicate the personal data breach to the data subject without undue delay.

1.2.8 Sustainability and Circular Economy

All the members of the data network are guided and incentivised to develop and deploy sustainable solutions in alignment with a more sustainable, circular economy. The members will implement the data network in a manner to make its operations more sustainable and circular, thus reducing its negative externalities on the environment, climate, and natural resources and avoiding doing significant harm to any stakeholder groups.

1.2.9 Transparency

The data network is based on co-operation and respect for information sources. Transparency is important to develop trust. The data shall be processed lawfully, fairly and in a transparent manner. Any information addressed to the public or to individuals must be concise, easily accessible and easy to understand, and clear and plain language and, additionally, where appropriate, visualisation is used. This does not mean that information is open to everybody without restriction. Instead, it means that all the members in the data network should know (when/if possible), what data are offered in the data network and by what requirements to promote transparency of network. To support real-time economy, the members of the data network do not unnecessarily detain data but share them as soon as possible.

The use of unnecessary legal jargon should be avoided. If an individual is asked to give a consent or to accept an agreement, it must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and using clear and plain language. Additionally, honest information should be provided to individuals for understanding what data regarding them is being collected and how it is being processed.

1.2.10 Continuous improving

Ethical issues vary and different issues may come up case by case. Thus, ethical evaluation should be a continuous process in organisation and there should be institutional support for this. Therefore, the management of a network member should support the organization's employees by ensuring that they have real opportunities to uphold, promote, and respect the principles of the Code of Conduct. Ethics is implemented in daily actions of individuals or it is not implemented at all, as only individual can make the moral decision. However, without institutional support for ethical decisions there is a higher risk of unethically as individuals lack the needed autonomy for being able to make moral decisions. The steering group has a mandate to follow up and develop the ethical model of the Traffic data ecosystem. The ethical maturity model will be in a development.

1.2.11 Support for individuals

All the members of the data network should support individuals in (a) getting information about use of their personal information, (b) understanding information, practices, contracts, and their consequences, and (c) participating, contributing, and influencing in systems and practices when using personal information of those individuals. The aim is to ensure that if individuals need information or have justified demands for Information, they are given needed support (Guidelines, personal help etc.) in transparent ways. The focus should be in creating low-barrier way to look overuse of personal information for those individuals from whom it is directly collected or other way received. However, the Traffic data ecosystem encourages individuals strongly to support adding value by using data responsibly.

1.2.12 Communication

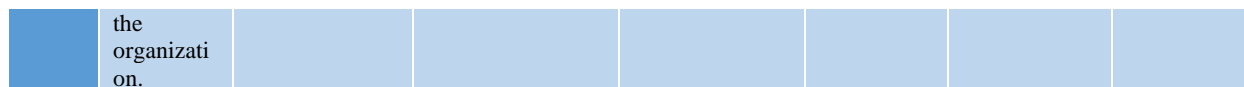
Appropriate communication is fundamental throughout the data network's life circle. It is essential for individuals, organizations, and the society as a whole. Each of them needs in addition to different contents and timing, also apposite communication channels and manners. A dialogue is a key way to build up trust in the network. The above-mentioned ethical principles are put into practice with communication. Furthermore, communication is the way to demonstrate the organization's commitment to them. The management has a special responsibility to articulate, apply, and support the organization's culture and processes that reflect the principles of this Code of Conduct.

1.3 Ethical maturity model

The maturity model presented in next page is tool that is developed to help organisation to evaluate its ethical maturity. However, it is developed such way that it would help the practitioners to have deeper view of situation in own organisation. Likewise, it provides conceptual and analytical tool that can be used to clarify the question "what should we do" by emphasising issues that needs not only to deal with but give deeper focus and considerations. Hence, the maturity model should not be seen as mere list of checkbox items, that is filled and forgotten. At best maturity model can serve as ground for discussion about organisational culture and values by providing different themes that help to start to critical self-investigation in personal and organisational levels.

Table 1. Ethical maturity model

	Security	Commitment to ethical practices	Transparency and communication	Sustainability	Human-centricity	Fair Networking	Purpose
Level 0	“I believe that this is very secure”	“We prefer not to commit, we are free”	“Just trust us”	“Let it burn”	“What this has to do with the people?”	“Anarchy”	“We do what we want to do”
Level 1	There are proper Antivirus, Firewall and other needed security tools in use and they are properly updated.	Organisation follows regulations and the best practices of its own field.	Organisation follows the regulations and uses truthful communication.	Organisation has documented sustainability plan/program.	The individuals are recognised as stakeholder and their rights are taken account.	Organisation aligns its rules and regulations to best practices of industry	Organisation has stated reasons for data collection and usage
Level 2	There is a dedicated person to keep up with information security.	Organisation has implemented and is committed to following ethical code(s) or other codes of conduct.	Organisation supports open internal communication and responsible information sharing.	There is an evaluation model for sustainability with clear indicators.	The organisation collects information of the needs of individuals to improve people-centricity.	Organization defines and documents practices and provides the needed information for network partners	Organization has transparent rules how data can be used in the future
Level 3	There are clearly documented procedures for the preparation of security threats.	There are clear well documented procedures for actions to be taken when ethical issues occur.	There is a transparent, documented plan for internal and external communication	Organisation impact on the environment is neutral or positive.	Individuals have low-level ways to communicate with the organisation and their opinions are systematically noted.	Organisation supports and encourages a fair data sharing in ecosystems.	The organisation negotiates with information sources to gain mutual understanding of fair information use
Level 4	The whole organisation has internalised the importance of security and it is constantly monitored and developed through	Organisational policies and procedures are developed critically from ethical perspective together with all relevant stakeholders.	Organisation and its representatives openly communicates its procedures and policies.	Organisation is actively advancing the sustainability of its business field.	Organisation will actively involve all relevant stakeholders in decision making.	Organisation actively seeks to ways to advance possibilities of whole ecosystems.	Organisation has clear, public, documented goals and procedure of information use



1.4 Further Material on Ethics

ACM code of ethics is ethical code that gives insights for computing professionals and managers to ethical issues that should be taken account in practice.

<https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf>

Ethics Guidelines for Trustworthy Artificial Intelligence by High-Level Expert Group on AI set up by the European Commission.

<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

Data ethics canvas provided by ODI (Open Data Institute) that focuses on helping identify and manage ethical issues of using data.

<https://theodi.org/wp-content/uploads/2019/07/ODI-Data-Ethics-Canvas-2019-05.pdf>

The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context

<https://www.eesc.europa.eu/sites/default/files/resources/docs/qe-04-17-306-en-n.pdf>